IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
WICHITA FALLS DIVISION

UNITED STATES OF AMERICA

v.

RICKY DALE HOWARD (01)

NO. 7:21-CR-008-O

CERTIFICATION OF DATA COPIED FROM AN ELECTRONIC DEVICE, STORAGE MEDIUM, OR FILE PURSUANT TO FED. R. EVID. 902(14)

I, Aaron K. Covey, attest under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by the Federal Bureau of Investigation (FBI) in the position of Special Agent assigned to investigate Crimes Against Children. I hold an FBI certification to conduct digital forensics. By reason of my position and specialized training, I am authorized and qualified to make this declaration as a "qualified person" under Fed. R. Evid. 902(14).

I further state:

1. The items I am certifying are Forensic Evidence Files ("FEFs"), also known as Forensic Images, obtained from the North Texas Regional Computer Forensics Laboratory ("NTRCFL"). On or about June 1, 2021 I requested the NTRCFL copy the following Forensic Evidence Files to a common network directory that I had access to:
   a. DL106752_1.E01
   b. DL108565_1.E01

2. Once these FEFs were copied to the common network directory, I copied these files, using TeraCopy version 3.8.5, to a Western Digital 3TB hard drive (**Government's Exhibit 56**).

3. I have been requested to verify the authenticity of these FEFs that I acquired from a common network directory belonging to the FBI and NTRCFL and copied to a Western Digital 3TB hard drive (**Government's Exhibit 56**). I have reviewed the FEFs that I copied to the Western Digital 3TB hard drive, below are the names and corresponding hash values of the FEFs that I am certifying:

   NTRCFL Forensic Evidence Files,

   a. DL106752_1.E01
      i. MD5 checksum: 998a819909b4a746192b35590bb58857
      ii. SHA1 checksum: f381e3fbd438022e8159ad1356b12c24dcfdf450
   b. DL108565_1.E01
      i. MD5 checksum: f26349afc7574598d7b57833b9a72dde
      ii. SHA1 checksum: dfda1edb9dff2bad2ce918fffa2cb70210728146

4. The hash values taken during imaging essentially runs each bit of data stored on the device through an algorithm (common algorithms include MD5 and SHA1) as it is copied onto the destination drive. This hash then serves as a digital "fingerprint" for the data, and may be verified at any time by running the data through the algorithm again. Verification that the data has not been altered in any ways is demonstrated when the resulting value is identical to the hash taken during acquisition.

5. For purposes of Fed. R. Evid. 902(14), I certify that **Government Exhibit 56** is an exact copy of the data that I acquired from NTRCFL via the network directory and that this data is authenticated by the above-referenced hash value, which is a process of digital identification.

I further state that this certification is intended to satisfy Fed. R. Evid. 902(14).

7/8/21

SIGNATURE DATE